나무위키

VeraCrypt

최근 수정 시각: 2026-08-02 16:27:51

분류:암호화 소프트웨어 | 오픈 소스 소프트웨어

목차

1. 개요
2. 특징
   2.1. 알고리즘
   2.2. UEFI와 GPT 지원
   2.3. 시스템 파티션 암호화 시 변경 사항
3. 사용 방법
   3.1. 응급복구 디스크
      3.1.1. 암호가 자꾸 틀리다고 하는 경우
      3.1.2. 윈도우 무한 자동 복구 준비 중
      3.1.3. 시스템 디스크 복호화하기
         3.1.3.1. 다른 컴퓨터에서 윈도우 복호화하기
4. 문제점
5. 관련 문서

VeraCrypt

개발자	IDRIX
발표일	2013년 6월 22일
플랫폼	Microsoft Windows, macOS, Linux, FreeBSD
라이센스	아파치 라이선스 2.0, TrueCrypt License 3.0

1. 개요

TrueCrypt 7.1a 버전에서 포크된 오픈 소스 암호화 소프트웨어. TrueCrypt가 개발 중단됐기 때문에 현재는 많은 사람들이 VeraCrypt를 쓰고 있다. 비영리 프로젝트로 개발 중이며, 이로 인한 수익은 오직 기부로만 받고 있다. 참고로 기부는 암호화폐로도 가능하다.

Linux, macOS, Windows에서 사용할 수 있고, https://veracrypt.io/en/Home.html에서 다운로드받을 수 있다.

2. 특징

VeraCrypt는 salt를 추가하는 등 TrueCrypt보다 보안성이 향상됐지만 대신 볼륨을 마운트하는 데 TrueCrypt보다 오래 걸린다.

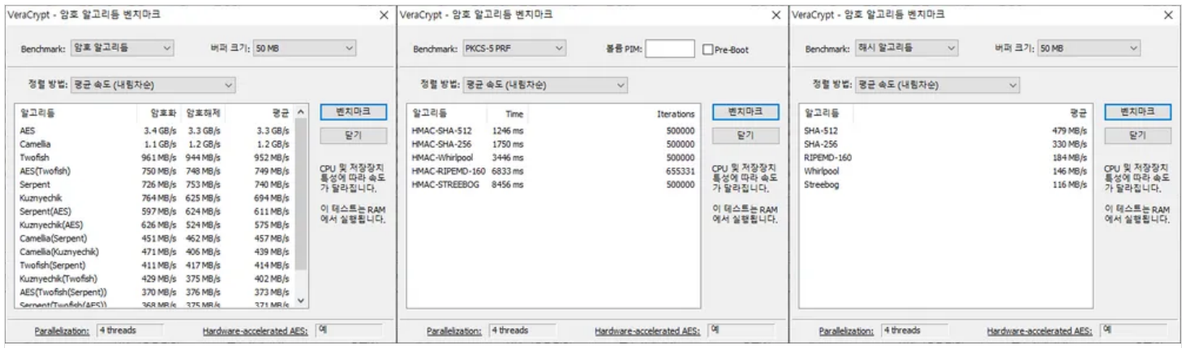
설치 파일은 한국어를 지원하지 않지만 소프트웨어는 한국어를 지원한다. 설치 이후 Settings -> Language...에서 한국어로 설정할 수 있다.

1.26.x 버전부터는 공식적으로는 윈도우 10부터 지원한다. 이전 윈도우에서도 계속 이후 버전의 VeraCrypt의 사용은 되지만, 새로 추가되는 기능에 대해 윈도우 8.1 이하에서의 테스트를 진행하지 않으므로 정상 작동이 계속된다는 보장은 없다.

Fast Startup(Fast Boot)은 비활성화하는 것을 권장한다.[1]

최신 버전에서는 Microsoft UEFI CA 2023 인증서로 서명되어 있어 보안 부팅을 지원하고 있다.

2.1. 알고리즘



브로드웰 + 32GB RAM에서 진행한 벤치마크. AES-NI 덕분에 AES가 압도적으로 빠르다. 보편적인 용도로는 AES-256 및 SHA-512 조합이 무난할 것이다.

- 암호화 알고리즘(Encryption Algorithms)은 AES, Serpent, Twofish, Camelia, Kuznyechik을 지원한다.
  - AES는 미국 정부 표준이며, Serpent와 Twofish는 AES 선정 당시 최종까지 후보로 남아있었다. Camelia는 일본에서 개발됐고, Kuznyechik은 러시아 정부 표준이다.

- 해시 알고리즘(Hash Algorithms)은 BLAKE2s-256, SHA-256, SHA-512, Whirlpool, Streebog를 지원한다.[2]
  - BLAKE2s-256은 2012년 12월 21일에 발표되어 VeraCrypt에서 사용하는 알고리즘 중에서는 가장 나중에 나온 알고리즘이다. 해시 충돌이 발생한 MD5와 SHA-1을 대체하기 위해 나왔다. SHA-2보다 뛰어난 보안성을 가지고 있고 특징이 SHA-3와 비슷하다. VeraCrypt에서는 256비트의 키를 만든다.
  - SHA-256은 NSA에 의해 개발되어 NIST(미국 국립표준기술연구소)에 의해 배포되었다. 2001년에 공개되었으며 256비트의 키를 만든다. SHA-512도 256과 동일하지만 키 파일 크기가 512비트이다.
  - Whirlpool은 2000년도에 빈센트 레이먼(Vincent Rijmen, AES의 공동 개발자)과 파울루 바레투(Paulo Barreto)에 의해 개발되었으며 512비트의 키를 만든다. VeraCrypt에서는 ISO/IEC 10118-3:2004 기준에 따른 세 번째 버전을 쓴다.
  - Streebog는 러시아 정부 표준이며 256비트나 512비트 키를 만들지만 VeraCrypt에서는 512비트 키만 만든다.

2.2. UEFI와 GPT 지원

윈도우의 C 드라이브 암호화는 BIOS와 MBR만 지원했었으나, 버전 1.18a부터는 UEFI와 GPT도 지원하기 시작했다.

2.3. 시스템 파티션 암호화 시 변경 사항

일반적인 부팅 과정 중에 VeraCrypt가 끼어들게 되므로, EFI 파티션에도 변화가 생긴다.

EFI 파티션의 **\EFI\Boot\bootx64.efi**, **\EFI\Microsoft\Boot\bootmgfw.efi**[3]이 변경된다. 각 파일은 같은 위치에 각각 original_bootx64.vc_backup 및 bootmgfw_ms.vc 이름으로 백업된다.

3. 사용 방법

[시스템 디스크 암호화 중의 안내 사항 원본 펼치기 · 접기]

예전에 TrueCrypt에서 만든 암호화 볼륨을 VeraCrypt에서 열려면 TrueCrypt Mode를 체크하고 마운트해야 한다. 다만 TrueCrypt에서 만든 볼륨의 마운트는 1.26.x 버전부터 지원하지 않으므로, 변환하지 않고 그대로 쓰려면 1.25.9나 그 이전 버전을 사용해야 한다.

간혹가다 볼륨을 마운트할 때 '장치가 준비되지 않았습니다'와 같은 오류가 뜨는 경우가 있는데, 이때는 명령 프롬프트를 관리자 권한으로 실행한 다음 mountvol /e를 치고 엔터를 누른 후 재부팅을 하면 해결된다.

VeraCrypt를 외장 하드/저장장치에서 숨겨진 볼륨과 함께 이용 시 **반드시 '매번' 수동으로만 켜야하는 숨겨진 볼륨 보호를 키도록하자**

만약 해당 옵션을 수동으로 체크하지 않는다면 표준 볼륨에 용량을 제한해둔 것과 상관없이 표준 볼륨의 파일이 숨겨진 볼륨으로 덮어씌워지게 되고,
이는 궁극적으로 숨겨진 볼륨 구성에 크랙을 발생시키는 요인이되고 **더이상 숨겨진 볼륨에 액세스할 수 없게 됨을 의미하며,** 이미 표준 볼륨 파일이 숨겨진 볼륨으로 넘어갔다면, TestDisk나 기타 복구 프로그램도 소용없다. VeraCrypt에서 자체적으로 지원하는 복구 옵션인 '볼륨 헤더 복원'도 마찬가지로 소용이 없다.~~나도 알고 싶지 않았다~~
위와 같은 일을 발생시키고 싶지 않다면, 항상 VeraCrypt가 적용된 저장장치에 표준 볼륨에서 과도한 용량의 파일을 저장하는 것을 피하고 그럴 수 없다면, 매번 숨겨진 볼륨 보호를 켜야 한다는 걸 까먹지 않도록 필히 주의하여야 할 것이다. 사실 애초에 숨겨진 볼륨 기능을 사용하는 경우 표준 볼륨은 "가짜" 기밀 정보를 저장하는 것이다. 즉, 정보를 저장하라고 만든 기능이 아니다. 숨겨진 볼륨 기능은 비밀번호를 말하도록 협박받는 상황에서 진짜 비밀번호 대신 가짜 데이터가 저장된 볼륨의 비밀번호를 대신 말할 수 있게 하는 기능이다.

숨겨진 볼륨 보호 기능을 사용하여 표준 볼륨에 파일을 저장하면 표준 볼륨 내에는 부자연스러운 빈공간이 발생할 수도 있다. 이 빈공간을 파악하여 히든 볼륨 존재를 확인할 수 있으므로 보호 기능의 사용에 유의할 것.

3.1. 응급복구 디스크

[4]

```
VeraCrypt rescue disk 1.25
d) Decrypt OS
m) Restore VeraCrypt loader to boot menu
z) Remove VeraCrypt loader from boot menu
c) Restore VeraCrypt loader configuration to system disk
k) Restore OS header keys
r) Restore VeraCrypt loader binaries to system disk
v) Boot VeraCrypt loader from rescue disk
o) Boot Original Windows Loader
h) Help
e) Exit
  [dmzckrvohe] :
```

각종 잘못 만들어진 프로그램, 일부 윈도우 업데이트나 BIOS(정확히는 UEFI) 업데이트 등으로 인해 방금까지 잘 사용하던 VeraCrypt 시스템 디스크로 부팅되지 않는 경우가 종종 생길 수 있다. 이러한 상황에서 디스크와 데이터를 살리기 위해 존재하는 것이 응급복구 디스크(VeraCrypt Rescue Disk.zip)이다. 갑자기 사용할 일에 대비해서 자신이 주로 사용하는 이메일이나 클라우드 스토리지에 저장해놓자[5][6]. 자신의 컴퓨터에 VeraCrypt 관련해서 오류가 갑자기 생긴 하면 PC방 등지에서 USB 메모리로 만들면 된다.

최신 VeraCrypt에서는 응급복구 디스크가 UEFI 환경에서만 가능하도록 바뀌었으므로, CSM 환경하에서 USB 메모리를 사용하려면 다음 링크의 하단을 참고하자. 다만 사전에 만들어둔 VeraCrypt Rescue Disk.**iso** 파일이 필요하다.

USB 메모리 만드는 내용은 마이크로소프트의 문서[7]를 참고하였다.

1. 먼저 부팅 가능한 USB 등의 외장 저장장치를 만드는 것이 필요하다. 비어있는 USB 메모리 등 저장장치를 컴퓨터에 꼽는다.
2. Windows 10 기준 **작업 표시줄** 검색창에서 cmd를 검색하고 우클릭을 해서 **관리자 권한으로 실행**을 클릭한다.
3. diskpart를 입력한 후 DISKPART>라고 뜰 때까지 잠시 기다린다.
4. list disk 혹은 lis dis[단축]를 입력한다. 자신이 사용하는 환경에 따라 다르니 **여기서부터는 용량 등을 재차 확인하면서 진행을 하는 것을 권장**한다.
5. 응급복구 디스크로 만들 디스크가 n번[9]이면 그에 맞춰서 select disk n 혹은 sel dis n[단축]을 입력한다.
6. clean 혹은 cle[단축]를 입력한다. **이때 응급복구 디스크로 만들 디스크가 지워진다.**
7. create partition primary 혹은 cre par pri[단축]를 입력하여 주 파티션을 만든다. select partition 1 혹은 sel par 1 [단축]을 입력하며 방금 만들어진 주 파티션을 선택하고 format fs=fat32 quick 혹은 for fs=fat32 quick[단축][15]을 입력하여 FAT32로 포맷[16]한다. 그다음 active 혹은 act[단축]를 입력하여 활성화한 후, exit 혹은 exi[단축]를 입력하여 diskpart를 종료한다.
8. VeraCrypt Rescue Disk.zip[19]를 방금 만든 드라이브 최상단에 압축 해제한다. 예를 들면 D 드라이브가 방금 만든 USB 메모리라면 D:\에 압축을 그냥 풀면 된다.
9. 제조사별로 정해진 방법에 따라 UEFI 환경에서 응급복구 디스크로 부팅한다.

3.1.1. 암호가 자꾸 틀리다고 하는 경우

VeraCrypt 마스터 키가 손상됐을 가능성이 있다. 응급복구 디스크에서 k[k]를 누른 후에 재부팅해 보자.

참고로 암호화 비밀번호를 바꾼 적이 있는 경우 각주에서 상술했듯이, 현재가 아닌 **이전** 응급복구 디스크가 있다면 이 메뉴를 이용해서, **이전** 암호로 디스크를 열 수 있다. 그러므로 비밀번호를 바꾸면 응급복구 디스크도 새로 만들고 이전 것은 바로 폐기하는 게 좋다.

주의할 점은 d[d]를 눌러 복호화한 후에 다시 k[k]를 누르면 암호화한 것처럼 인식이 되어 디스크가 망가지게 된다. 따라서 복호화한 디스크에 k[k]를 누르는 일이 없도록 하자.

혹여, 애초에 비밀번호를 잘못 작성하여 복호화가 불가능하거나 키 파일이 변경, 제거되는 등 손실이 일어나면 암호화된 디스크는 절대로 복호화나 복구가 불가능하다고 보면 된다. 가장 기본적인 AES 암호화도 현존하는 최고의 슈퍼컴퓨터는 물론 양자컴퓨터를 가져와도 해독하는 것이 불가능하다고 여겨진다. 즉, 디스크를 포맷하고 데이터를 모두 날리는 방법밖에 없다. 포맷 후 데이터 복구를 시도해 봤자 어차피 복구된 데이터도 암호화된 상태니 의미가 없다.

3.1.2. 윈도우 무한 자동 복구 준비 중

윈도우가 설치된 디스크를 암호화하면 부팅 과정에 VeraCrypt 부트로더[24]가 관여하게 된다. 이 부트로더를 거치치 않으면 윈도우에 접근이 안 되며, VeraCrypt가 관여하지 않고 바로 윈도우 부트 매니저로 부팅하게 될 일이 생기면 자동 복구 준비 중 화면을 보게 된다. 이것은 정상적인 것으로, 암호가 입력되지 않았으므로 기존의 윈도우 부트 매니저

는 읽을 수 없어 고장 난 윈도우로 인식하게 되므로 원인을 알 수 없어 무한하게 자동 복구를 시도하는 것이다.[25]

이 화면을 자주 볼 수 있는 때가 바이오스를 업데이트하였을 때이다. 바이오스 업데이트를 하면 대체로 설정이 초기화가 되는데, 설정된 부팅 순서도 초기화가 되면서 VeraCrypt 부트로더가 아닌 기존의 윈도우 부트 매니저를 로딩하면서 오류를 뿜는 것이다. 간단하게 바이오스의 해당 설정에서 VeraCrypt 부트로더를 먼저 읽게 순서를 바꿔주면 해결된다. [27]

바이오스(UEFI)에서 VeraCrypt 로더가 아예 나오지 않는 증상도 발생할 수 있다. 이 증상에는 2가지 경우가 있는데, 첫 번째는 단순히 바이오스 메뉴에서 보이지 않는 것[28] 그리고 두 번째는 VeraCrypt 로더 자체가 날라간 것이다. 전자의 경우, 응급복구 디스크로 부팅한 후, m[m]을 누르고 재부팅하고 바이오스에 들어가면 부팅 순서에 VeraCrypt 로더가 생겨있는 것을 볼 수 있다. 후자의 경우, 단순히 순서가 아니라 VeraCrypt 부트로더가 망가지거나 날라갔다면[30], 응급복구 디스크로 부팅한 후에 r[r]을 누르고 m[m]을 누르면 간단히 해결된다.

3.1.3. 시스템 디스크 복호화하기

데이터 자체에 손상이 가지 않은 이상, 대부분의 문제는 복호화(d[d])하고 VeraCrypt 로더를 없앤 다음(z[z]) 기존의 윈도우 부트 매니저로 부팅하면(o[o]) 거의 해결된다.

3.1.3.1. 다른 컴퓨터에서 윈도우 복호화하기

응급복구 디스크가 있으면 윈도우가 고장 나서 진입이 안 되는 등의 상황에서, **대상 VeraCrypt 디스크의 비밀번호를 안다는 전제하**에 다른 PC에서 복호화를 할 수 있다. 당연하지만 비밀번호를 모르면 복호화가 불가능하다.

응급복구 디스크로 부팅한 후, d[d]를 누르고 복호화할 윈도우가 고장 난 VeraCrypt 디스크가 탑재된 저장장치를 컴퓨터에 연결하고, 그 비밀번호(있다면 PIM까지)를 입력한다. 평소 부팅 때와는 달리 암호 입력 후에 딜레이가 조금 오래 걸리므로[37][38] 조바심을 갖지 말고 기다리자. 암호가 맞다면 해당 드라이브를 복호화할지 Decrypt? 라면서 물어본다. y를 누르면 복호화가 진행된다. ETA가 계산상으로는 며칠~몇 주가 나오지만 실제로는 한두 시간 이내에 복호화가 완료된다. 중간에 esc 등을 누르면 Stop?이라고 묻는데 n을 누르면 하던 작업을 이어서 한다.

복호화 후에 z[z]를 눌러서 UEFI에서 VeraCrypt 부트로더를 인식 못 하게 한 후(시스템에 따라 나중에 UEFI의 부팅 순서에서 Windows Boot Manager를 최상단으로 올려준 후에), o[o]를 눌러서 윈도우 부트 매니저로 부팅을 하면 암호화 이전의 상태처럼 암호 입력 없이 암호화되지 않은 평범한 윈도우에 진입하게 된다.

상술했듯이 복호화를 완료한 후에 실수로 k[k]를 누르게 되면 암호화가 된 것처럼 인식시켜버리므로 키보드 키를 누를 때 조심하자.

4. 문제점

간혹 부트로더가 날라가서[42] 블루스크린이 출력되는[43] 경우가 있어 주의를 요한다. 특히 (바이오스라고 자주 불리는) UEFI 업데이트가 잦은 최신형 시스템에서 VeraCrypt 부트로더가 사라지는 일이 자주 발생할 수 있으니 응급복구 디스크를 미리 만들어두고 메일 등에 응급복구 디스크를 백업해놓자. 상술했지만 비밀번호를 모르면 **절대**로 복호화를 못 하므로 백업을 많이 해주는 것이 좋다.

윈도우 10에 11로 올리는 등의 업그레이드 시에는 **반드시** 영구 복호화 후에 업그레이드하여야 한다. 업그레이드 과정에서 암호화된 시스템 디스크 설치 프로그램이 읽을 수 없어 오류가 발생하게 된다. 이미 업그레이드를 진행해서 오류가 발생하였을 때에는 미리 만들어둔 응급복구 디스크를 통해서 부팅하면 업그레이드 이전으로 자동적으로 윈도우가 알아서 복원 과정을 진행한다. 그리고 그 이후에 윈도우 11 업그레이드를 재시도하면 높은 확률로 0xc190012e 오류가 발생하는데 **C:\Users\Default\AppData\Local\Microsoft\Windows\WSUS** 위치에 있는 **setupconfig.ini** 파일을 삭제하고 재부팅한 후에 진행하면 된다.[44]

Windows를 사용해야만 할 경우 안정성을 위해 LTSC(장기지원) 버전을 채택하는 것이 도움이 될 수 있다. Windows 10 Enterprise LTSC[45]나 Windows 11 Enterprise LTSC[46]처럼 장기지원버전을 사용하면 메이저 업그레이드로 인한 불상사를 피할 수 있다. 이들은 장기지원이라는 그 자체도 장점이지만, 일반 Pro나 Home버전처럼 자기 멋대로 메이저 업그레이드를 수행하지 않는다. 서버나 워크스테이션 등 산업용 제품을 목표로 출시되었기 때문.

하드웨어 가속인 AES-NI를 지원하는 프로세서라면 AES 사용 시 체감 속도 저하를 거의 느끼지 않은 채로 사용이 가능하다. 다만 AES-NI가 있어도 기술 발전에 따른 성능 자체의 격차는 있기 때문에, 구형 시스템에서는 VeraCrypt를 버티지 못 하는 경우가 종종 발생할 수 있다.

5. 관련 문서

- TrueCrypt
- FileVault
- CipherShed
- Cryptomator
- salt

이 저작물은 CC BY-NC-SA 2.0 KR에 따라 이용할 수 있습니다. (단, 라이선스가 명시된 일부 문서 및 삽화 제외)
기여하신 문서의 저작권은 각 기여자에게 있으며, 각 기여자는 기여하신 부분의 저작권을 갖습니다.

나무위키는 백과사전이 아니며 검증되지 않았거나, 편향적이거나, 잘못된 서술이 있을 수 있습니다.
나무위키는 위키위키입니다. 여러분이 직접 문서를 고칠 수 있으며, 다른 사람의 의견을 원할 경우 직접 토론을 발제할 수 있습니다.